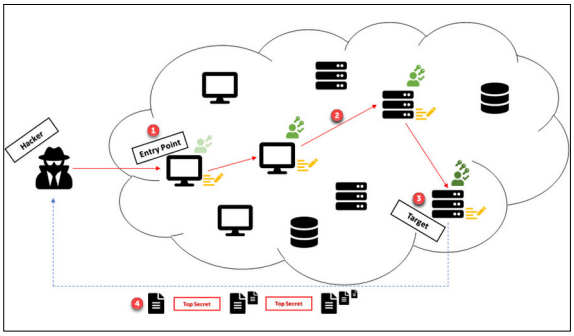

Claudio Mattes


Lukas Kellenberger

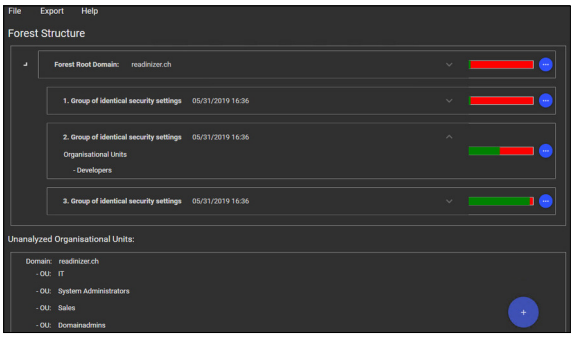
Graduate Candidates	Claudio Mattes, Lukas Kellenberger
Examiner	Cyrill Brunschwiler
Co-Examiner	Dr. Christian Folini, netnea AG, Liebefeld, BE
Subject Area	Security

Readinizer

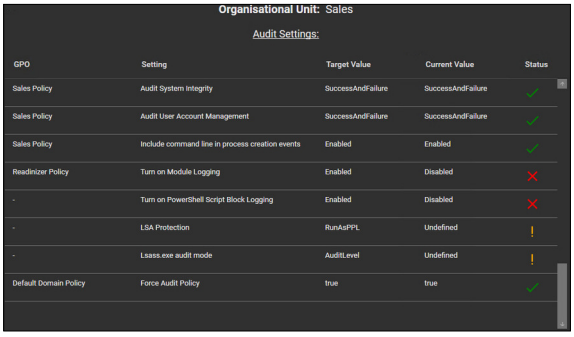
Readiness Analyzer, Visualizer and Optimization



Overview of a lateral movement / APT attack
Readinizer, 2019



Forest structure with analysed groups of identical security settings
Readinizer, 2019



Detailed view of security settings within an OU
Readinizer, 2019

Introduction: The number of cyber-attacks where malicious code is used has massively increased recently. These attacks not only settle on the infected system, but can also infect other systems through lateral movements in the network. The outcome is often the complete infiltration of the organization due to the use of advanced persistent threats (APT). Although the configuration of these targeted networks varies depending on the organization, common patterns in the attack methods can be detected. In the analysis of such patterns and events, information and time are key factors to success. Hence, readiness and a fast access through an entire environment for such an event is a decisive factor.

Approach: The main aspect of this project was to analyze readiness of the configured settings - through an entire Active Directory (AD) environment - and give a statement to improve those. On the other hand, but still with a significant importance, an optimization part was planned to improve the present state of the environment. In a first step, a benchmarking of the defined recommended audit settings from the previous Proof of Concept (PoC) was performed against several Computer Emergency Response Teams (CERT) all over the world. Simultaneously, architectural and design decisions for the application have been made. After further research in upcoming topics, the construction of the application "Readinizer" for the analysis part was performed. The construction phase also contained the optimization part. Last but not least, manuals for the application and the entire project have been documented.

Result: The application ``Readinizer'' analyzes an entire AD forest and gathers information about all domains, sites, organizational units (OU) and member computers/servers. As soon as this information is gathered and all relationships between these objects are resolved, the "Readinizer" calls one computer/server of each OU to receive a Resultant Set of Policies (RSoP). A RSoP is a summary of the applied computer settings that were made locally or distributed via group policy objects (GPO). Since an OU has the highest precedence when applying GPOs, it is sufficient to query only one computer of each OU. Then an analysis is performed for each received RSoP, comparing the current settings in the AD forest with the recommended settings - based on the benchmark. The result of the analysis is then presented to the user in form of a percentage figure whereby a tree structure of the forest depicts the analyzed RSoPs and gives a first view of the readiness. In addition, the user has the possibility to simultaneously perform a Sysmon check. Sysmon is a tool by Mark Russinovich which logs the same events as the default event logger but where the executables are hashed. Hence, compromisation of such executables can be detected. The user can then drill down the RSoPs to a detailed view over all applied / recommended settings and which GPO applied those settings. With the optimization part of the "Readinizer", the distribution of Sysmon to an entire fleet is simplified for the user, as well as the setup of central logging by Windows Event Forwarding - with appropriate templates - is made available in the form of manuals. The "Readinizer" also includes a GPO of recommended settings which can be imported.